(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number
WO 02/25436 A2

(51) International Patent Classification[7]: G06F 9/445

(21) International Application Number: PCT/GB01/04174

(22) International Filing Date:
19 September 2001 (19.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0023177.9 21 September 2000 (21.09.2000) GB

(71) Applicant *(for all designated States except US)*: **WORK4SURE.COM LTD.** [GB/GB]; Millfield House, Cropwell Road, Radcliffe on Trent, Nottingham NG12 2JG (GB).

(72) Inventors; and

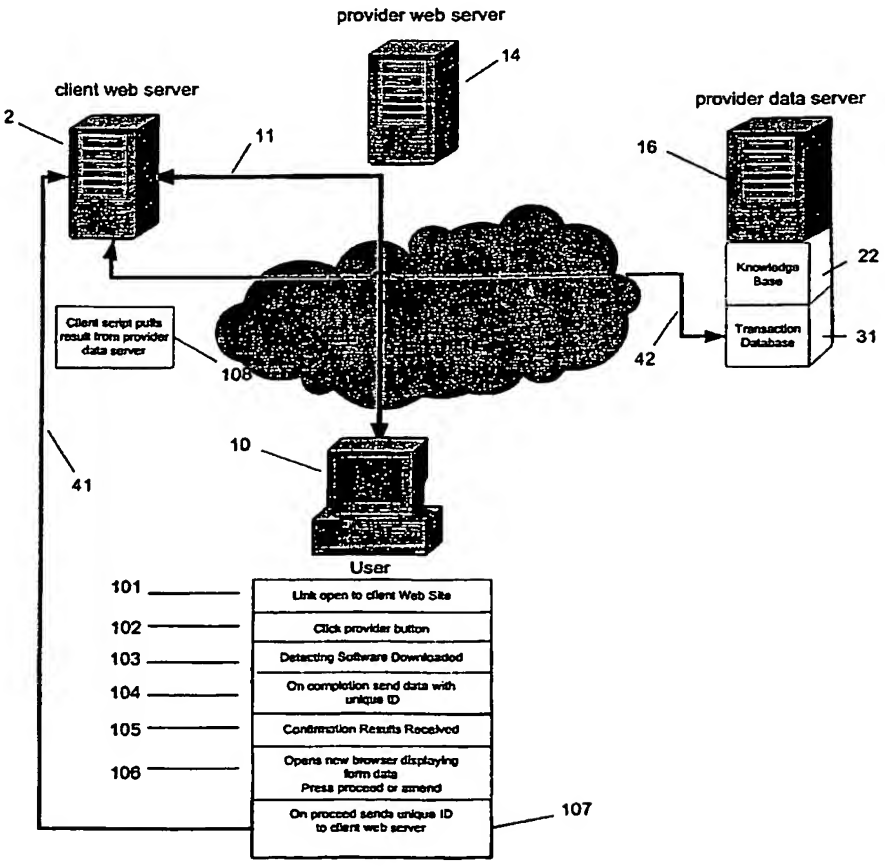
(75) Inventors/Applicants *(for US only)*: **MIRYANOV, Vitaly** [UA/GB]; 209 Sandycombe Road, Kew, Richmond, Surrey TW9 2EW (GB). **BATEMAN, Liam, Peter** [GB/GB]; 7 Shipps Close, Harleston, Norfolk IP20 9BG (GB). **FESSEY, Damian, Robert** [GB/GB]; Millfield House, 74 Cropwell Road, Radcliffe on Trent, Nottingham NG12 2JG (GB). **SHELDON, Andrew, David** [GB/GB]; Hall Barn, Westhorpe Road, Wyverstone, Suffolk IP14 4SP (GB). **LLOYD-ROACH, David, Joseph** [GB/GB]; 3 St. Mary's Walk, Ardley, Oxon OX27 7PR (GB).

(74) Agent: **CHARIG, Raymond, J.**; Eric Potter Clarkson, Park View House, 58 The Ropewalk, Nottingham NG1 5DD (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI,

[Continued on next page]

(54) Title: REMOTE COMPUTER CONFIGURATION SCANNING



(57) Abstract: A system for detecting and forwarding, across the Internet to a third-party, configuration data detected from a user's computer, which user is a visitor to the third party's web site. In one configuration, apparatus for the remote scanning of configuration data relating to hardware or software installed in or as part of a user's computer system includes means for downloading a software-based scanning module from a provider's server to a user's computer system, the scanning module including means for determining preselected items of configuration data from the user's computer system and conveying said configuration data to the provider's server, and means for forwarding said configuration data to a client's server. The pre-selection of items of configuration data to be collected may be predetermined by the client to the provider. The user may be enabled to verify and authorise the forwarding of the information to the client's server by the provider's server.

WO 02/25436 A2

BEST AVAILABLE COPY

SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

BNSDOCID: <WO_____0225436A2_I_>

REMOTE COMPUTER CONFIGURATION SCANNING

The present invention relates to systems for the remote sensing of the configuration of computer system hardware and software.

Use of the Internet to obtain products and services from retailers' web sites on the Internet (hereinafter "e-tailers") is becoming widespread. Purchasing products and services in this way removes or restricts an important element from the purchasing transaction – that of obtaining advice on the suitability of the product or service to be purchased. As an illustration, suppose that an anonymous web-surfer wishes to purchase a webcam for his computer from an e-tailer. The e-tailer offers a wide range of webcams from different manufacturers, each of which is targeted at different needs, which are dependent on:

(1) what the visitor wishes to use his webcam for, ie. his buyer preferences; and

(2) the technical specification of his computer, ie. what his computer is capable of running or is compatible with).

However the e-tailer's breadth of offering is of little value to either party unless the options within the range can be matched to the needs of the individual consumer in this e-tail environment.

Establishing the web-surfer's buyer preferences can be relatively easy via a web page: the e-tailer can simply present him with a pick list describing possible preferences, and ask him to select the one which (most closely) describes his preference.

Where it becomes more difficult is in terms of technical specification. The reality is that most computer users are unable to provide even the most basic details about their computer reliably and accurately. In any case, in many situations, it is the detail that matters. Selling a USB-connecting webcam to a Windows 95 user is of little use unless the user is running Windows 95 versions B or C (which have USB support) as opposed to version A (which doesn't).

BNSDOCID: <WO_____0225436A2_I_>

Quite apart from the purely technical aspect of ascertaining the computer specification, there is also the human element to consider. Asking a user a question to which he or she is unlikely to know the answer effectively raises barriers to a sale at exactly the point in the sale process where the objective is to remove any remaining barriers to the sale. It is expensive and counter-productive to address such questions to the users when the questions could be addressed directly to the computer itself with much greater speed, accuracy and efficiency.

It would therefore be desirable to automatically detect the hardware and/or software configuration of a users computer system prior to offering computer products or services for sale.

A number of hardware- and software-based computer inventory tools which are designed to detect personal computer configuration data are known in the art. Typically these products are used to conduct audits across a population of PC's or to collect data to populate applications such as asset management programs. Invariably, the inventory tools collect more than the hardware configuration data and are sizeable executables that generate large data files.

Typically, inventory programs are executed from floppy disk or from a server on a network, and the resulting data file is either saved back to floppy disk or the server. These inventory programs are not optimised for use across the Internet where the download time for the program and the subsequent upload time of the saved data would be prohibitive. The present invention is directed rather to a system which is particularly suited to computer hardware and software detection across the Internet and which requires no specialist knowledge on the part of the user.

A further problem is a question of trust in the relationship between the user and the prospective vendor. Many users may have a reluctance to agree to the unrestricted scanning of their computer system by a commercial organisation that is primarily concerned with making sales.

BNSDOCID: <WO_____0225436A2_I_>

A further problem is that an e-tailer is concerned primarily with the sale of goods and services and does not necessarily have the expertise or the wish to acquire and maintain expertise in sophisticated computer scanning systems.

An objective of the present invention is therefore to provide an automated system for matching a user's technical needs with appropriate hardware and software systems which are available for purchase via an e-tailer's web site.

A further objective of the present invention is to provide an attachment technology for e-business by which, via their web site, a client e-business can enable the automatic examination of a visitor's computer (or other Internet-connected device) to determine the specification of that device and its suitability to receive products and services marketed by that e-business.

A further preferred objective of the invention is to provide a system in which can lie between a vendor of hardware or software and a prospective purchaser to match the requirements of the two parties while being independent of both.

Some or all of the above objectives are met with various embodiments to be described herein.

According to one aspect, the present invention provides a hardware and software system and method to detect and forward across the Internet to a third-party, configuration information detected from a user's computer, which user is a visitor to the third party's web site.

The operation of the system is initiated by the user, from the web site of the third-party. The system comprises the software tool(s) for detecting the configuration information, the means for establishing the channels of communication between the third-party, user and a server on which the software tools and detected data are stored, and the return of validated data to the third-party.

BNSDOCID: <WO_____0225436A2_I_>

According to another aspect, the present invention provides apparatus for the remote scanning of configuration data relating to hardware or software installed in or as part of a user's computer system, the apparatus comprising:

means for downloading a software-based scanning module from a provider's server to a user's computer system;

said scanning module including means for determining preselected items of configuration data from the user's computer system and conveying said configuration data to the provider's server; and

means for forwarding said configuration data to a client server.

According to another aspect, the present invention provides a method of remote scanning for configuration data relating to hardware or software installed in or as part of a user's computer system, the method comprising:

determining preselected items of configuration information required;

initiating, by a user, download of a scanning module from a provider's server to the user's computer system;

determining, by said scanning module, configuration data for said preselected items of configuration information from the user's computer system and conveying said configuration data to the provider's server; and

authorising, by said user, transmittal of said configuration data to a client server.

According to another aspect, the present invention provides a method of verifying compatibility of a user's computer system with at least one candidate product or service comprising the steps of:

visiting, by a user, a client web site;

initiating, by the user, download of a scanning module from a provider server by activation of an address embedded in the client web site;

scanning the user's computer system using said scanning module;

forwarding configuration data resulting from the scan to the client server.

Embodiments of the present invention will now be described by way of example, with reference to the accompanying drawings in which:

BNSDOCID: <WO_____0225436A2_I_>

Figure 1 shows a schematic diagram of the various components of a computer networked system suitable for carrying out the invention, and indicating data flows involved in an initial stage of a scanning operation;

Figure 2 shows a schematic diagram of the system of figure 1 indicating data flows during a second stage of a scanning operation;

Figure 3 shows a schematic diagram of the system of figure 1 indicating data flows during a third stage of a scanning operation;

Figure 4 shows a schematic diagram of the system of figure 1 indicating data flows during a fourth stage of a scanning operation;

Figures 5 to 9 show schematic diagrams of the system of figure 1 indicating data flows during stages of an alternative scanning operation.

Throughout the present specification, the person using the computer system which is to be examined or scanned for configuration data will be referred to as the "user". References to the user's computer system are intended to include any type of network-connected (and in particular, Internet-connected) processing device, which may include Internet television set-top boxes and the like. The e-tailer or other business that is operating a network device, eg. web server, by which products and services are being sold to the user will be referred to as the "client", and references to the client's web server are intended to include any network-connected computer devices which require configuration data to be received in respect of a user's computer system. A third network-connected computer system that is providing the computer scanning service to be described herein is referred to as the scanning system "provider".

Although a preferred embodiment is described in the context of a commercial environment in which an e-tailer is selling products or services which require a knowledge of the user's computer system, it will be understood that the invention is not limited to use in such a commercial environment.

The configuration data being scanned from the user's computer may include both hardware and software configuration data. In general the configuration data may comprise a detailed description of the internal hardware components of the user's computer system, a detailed description of peripherals attached internally or

BNSDOCID: <WO_____0225436A2_I_>

externally to the computer system, together with a detailed description of the software (eg. operating system, applications and drivers) installed on the computer system. The detailed description may include the make and model of the component and/or peripheral, or the publisher, name and build standard of software. The detailed description may also include information on the speed, storage capacity, quantity of memory and means of connectivity of the hardware component and/or peripheral as appropriate to its function. The detailed description is not necessarily limited to the items described above. Preferably, the configuration data collected is customised to the needs of the client or client server, eg. in accordance with the products or services the client is trying to sell.

The system of the present invention is preferably optimised for efficient information collection from the user's computer system, in particular over a limited bandwidth network such as the Internet. This is achieved by making the system fully configurable to collect only the targeted information. The information collected may be verified against a comprehensive and extensive data set maintained in the provider computer system to ensure accuracy. The technology can be readily adapted to operate across a broad range of computer operating systems to include all variants of 32-bit Microsoft Windows™ platforms, Apple Macintosh™ and other operating systems. The data collection capability can be comprehensive and extensive. In the preferred embodiment, the system is easy to configure by clients and easy to operate by the end user.

A significant feature of the preferred embodiment of the present invention is that a three party system, namely (i) computer user (eg. private individual); (ii) client (eg. e-tailer, or other e-business) and (iii) provider (of the scanning service) enables the provider system to be completely independent of the client system. Thus, the provider of the computer scanning service may be a trusted third party who can give assurance regarding user data privacy ensuring that only relevant configuration data is collected and passed to the client, and can build a comprehensive knowledge database of computer system configuration types.

Another significant feature of an embodiment of the invention is that the scanning code does not carry the burden of databases to match the detected raw configuration

BNSDOCID: <WO_____0225436A2_I_>

data with. Data matching is achieved by passing raw configuration data back from the user's computer to a data server for processing. This enables very compact scanning code sequences to be used which result in quick and easy transmission using standard Internet transmission protocols.

The system of the preferred embodiment is made up of a number of components that combine to form a coherent and flexible product that dynamically adapts to the information requirements of a client and a user. There are four basic stages, each making use of a series of components as follows:

(a) Initial configuration

The initial configuration process is used by the client to specify which data is to be collected from the user's computer system. This is preferably performed by filling in a web-based form. The result of this initial configuration process is a personalised uniform resource locator (URL) that is placed on the client's web site.

(b) Initiation

A scan is initiated when a user clicks on this URL on the client web site. The URL calls and downloads an executable piece of code from the provider computer system.

(c) Scanning

The raw hardware and configuration data is detected in the user's computer system and then passed to the provider's application server for further processing and identification using a predetermined knowledge base in the provider's server.

(d) Delivery

Once identified, the required configuration data is made available to the client server for further processing.

Initial configuration

Preferably, the system is first configured for use, by the client, via a web page on the provider's web site. The client may identify the configuration data items that it wants to detect on the user's computer system by selecting them from drop-down

BNSDOCID: <WO_____0225436A2_I_>

hierarchical menus. Thus the data set required may be unique or customised to each individual client. Once the initial configuration process is completed, the client will be presented with a confirmation of the data items selected and a textual URL link to the provider's server, which the client can incorporate into the hypertext mark up language (HTML) on their web pages. Thus, in this fashion the system more generally provides a means for, remotely from the client server, preselecting required items of configuration data and storing said required items' definition in the provider's server.

In a preferred embodiment, a script will also be incorporated into the client's web page which will display the provider's URL "button" which may be clicked by the user to establish the required link to the provider's server. The URL link also contains a unique client identifier (UCI) that is used to direct the results of a scan of the user's computer system to the correct client web site.

Thus, while in the preferred embodiment, the preselection of configuration data items required is implemented remotely from the client server, the initial configuration process could be carried out in a number of other ways. These could include, for example, direct programming at the provider's server. This process, being a relatively infrequent operation, need not be carried out on-line over the Internet but could be carried out using other conventional information submission methods.

Once the configuration process is complete and the URL link incorporated into the client's web page the system is ready for use.

Operating sequence

With reference to figure 1, a user 10 establishes a link 11 with a client web server 12 by visiting the client's web site (step 101) and will see the provider's button that will launch the data detection or scanning process. Once this button is pressed (step 102), a link 13 is established between the user's computer system 10 and the provider's web server 14 and the detection / scanning software is downloaded to the user (step 103) from the provider's web server 14. The detection / scanning software downloaded to the user is preferably customised to scan only for the

BNSDOCID: <WO_____0225436A2_I_>

configuration data required according to the initial configuration request of the client.

With reference to figure 2, the detection / scanning software runs and establishes a link 21 with the provider's data server 16. Once the scan is complete, the detected configuration data will be identified with a unique ID, possibly generated from session data, and then passed (step 104) to the data server 16 knowledge base 22 for verification. Compression algorithms may be used on the data packets sent to the provider's data server from the user's computer system.

Confirmation of receipt of the configuration data will be passed back (step 105) to the user's computer system on link 21. In a preferred embodiment, to ensure complete confidentiality of information, no personal information would be included in the detected data and the user will remain unidentifiable. For example, system specific information such as the Intel® CPU serial number might be excluded from collection.

With reference to figure 3, the configuration data is stored as a unique record in a transaction database 31 on the provider's data server 16. Once confirmation is received by the user's computer system that the data has been stored correctly, the user will be invited to view the information detected. If the user chooses, the detecting / scanning software displays the results, for example, by opening a new browser displaying the data in a form (step 106).

At this stage, and depending on the initial configuration of the system, the user may be allowed to amend details in designated fields on the form. To achieve this, there is provided a means adapted to enable the user to edit the configuration data displayed on the user's computer system and thereby to enable the user to edit the configuration data stored in the transaction database. This will typically be used where user's PC make and model information is requested by the client but is undetectable on the user's PC.

BNSDOCID: <WO_____0225436A2_I_>

In one embodiment, where the user decides to edit the configuration data, a further communication may be commenced between the user's computer system and the provider's data server to complete this function (not shown).

With reference to figure 4, the user will then be invited to confirm that the configuration data presented can be passed to the client web server. To achieve this, there is provided a means for enabling the user to confirm or inhibit passing of configuration data to the client server. In the example, the user may click a button to authorise the transfer of the configuration data to the client web site (step 107). By this action, the user computer 10 sends a unique identification code for the information to the client web server on link 41, and the client script uses this code to pull the scanning result from the provider's data server 16 on link 42 (step 108). The preferred default data format is extensible mark up language (XML) although other formats may be provided such as Management Information Format (MIF) or plain HTML.

Alternatively, the user may be given the opportunity to cancel the operation and prevent any configuration data being passed to the client web site.

Once the configuration data is received by the client web server 12 it can be processed in a number of ways. Sample PERL or active server page (ASP) scripts may be provided to clients by the provider giving examples of decision tree methods and similar actions to be taken using the data. Generally speaking, the client is not required to install any bespoke software to read the results detected from the user computer system.

In the preferred embodiment, these may be used to control the selection of data presented to the user 10 on the client's web page. For example, the number of available hardware or software items presented for sale may be restricted to purchase options which are technically suitable, ie. with which the user's computer system will be compatible.

Thus, in the preferred embodiments described above, the invention provides a computer configuration detection system optimised for use across the Internet. It

BNSDOCID: <WO_____0225436A2_I_>

will be understood that the invention is applicable to other computer communication networks.

In preferred embodiments, the configuration detection system is capable of detecting in excess of 300 items of hardware configuration including: type and speed of CPU; installed RAM; number of, capacities of, and free space on hard drives; graphics card make, model and video modes; BIOS manufacturer and version; interfaces installed and in use; modem and network card makes and models; network protocols and addresses and more.

The configuration detection system is optimised for use over the Internet by keeping the downloaded scanning software code as small as possible for the task in hand. By providing an initial configuration step in which clients determine what they require in the way of user's configuration data, only the data required is downloaded from the user's computer.

The scanning software code is preferably downloaded onto, and configuration data uploaded from, the user's computer using standard Internet protocols.

Preferably, there shall be no legacy code or data left on the user's computer. All downloaded scanning code may be cached and thus erased when the cache is either erased or rotated. Alternatively, the downloaded scanning code may be auto-deleting. This avoids any permanent legacy data or indication of the data detection on the user's computer. However, cookies could be employed to track the visit to the provider's web server site.

In the preferred embodiment, the scanning / detection is conducted while the user is still connected to the client's web site and is essentially part of that connection session as it is integrated into the user's visit to the client web site.

Advantageously, the preferred embodiments of the system require minimal understanding and intervention on the part of the user. All the user has to do is click the provider's button on the client's web site to launch operation of the system. Preferably, the transactions between the user and the provider are subject to

BNSDOCID: <WO_____0225436A2_I_>

authentication and integrity checking procedures, such as those provided by a third party, such as VeriSign. The initial download of code onto the user's computer may use VeriSign technology to maintain integrity.

The initial stages of configuration data detection or scan may include a multi-stage procedure to determine how best the information can be detected. An iterative interaction between the user's computer and the provider's data server is possible to determine the course of action for the detection. The detection process may incorporate a detection hierarchy. Detection would initially (via the first module downloaded) follow a logical path of looking at targeted areas of the system for specific information, for example the System Management BIOS data. Should the information not be found in these targeted areas, or should the system not support the protocol, further data detection would take place possibly utilising other modules that would be downloaded onto the end-user's computer.

The system may be designed to work with systems running 32-bit versions of Microsoft Windows™ on platforms accessed across the Internet or for Apple Macintosh™ and other operating systems. The system may be designed to collect data from all generations of computers capable of running these operating systems.

The detection / scanning software is preferably downloaded to the user's computer using standard Internet protocols. The software preferably specifies the items of configuration data required by the client, and once downloaded, self-executes on the user's computer and establish a link to the provider's data server. The software then detects the required data set corresponding to the items of configuration data specified.

In the event of encountering an unknown computer whose configuration data the scanning software cannot detect, the provider's server may be adapted to download from the user's computer whatever data is needed to build a comprehensive picture that will be used to constantly update the provider's knowledge database.

Where there is ambiguity in the configuration data, the ambiguity may be notified to the user and / or the client.

BNSDOCID: <WO_____0225436A2_I_>

In a preferred embodiment, the provider and the provider's servers will be operated by a different commercial entity to the operator of the client's servers. The system may provide for the maintaining of billing information related to the number of accesses by users for the provider's scanning services, so that the client entity can be billed accordingly by the provider entity. Cookies may be used to record the use of the service. These cookies may be unique to each client (eg. linked to their specific URL calling the detection tool). If a user were to revisit the site within a predetermined period of time, eg. 24 hours, the configuration data may be re-detected but not counted for invoicing purposes, or may be not counted for invoicing services providing that the configuration data remains unchanged since the last configuration scan. Alternatively, billing information may generally be collected on a per hit or time period-based system.

Preferably, a unique ID will be generated on each execution of the scanning software. This will be used to link the information detected with the session. Preferably, the algorithm for generating the unique ID will not make use of any personal information.

Preferably, each URL link generated by a client will contain a unique identification code allowing the client to place a number of different provider buttons on their site to perform different categories of data collection and subsequent processing. For example, one link might assist users wishing to purchase memory. The configuration data collected for this scan could direct the user to the appropriate memory products. Another scan may be used to identify which CPU would work in the computer as an upgrade from the current CPU.

To optimise the size, and speed of download and execution of the detection component of the scanning software, the system may use a control stub that, once downloaded onto the end-user's computer, will call down additional executable modules to conduct the detection. The control stub may contain a description of the items required to be detected. The modules may be called down in sequence with the results from the execution of one used to determine whether additional modules are required.

BNSDOCID: <WO_____0225436A2_I_>

The detection process may incorporate a detection hierarchy. Detection would initially (via the first module downloaded) follow a logical path of looking at targeted areas of the system for specific information, for example the System Management BIOS data. Should the information not be found in these areas, or should the system not support the protocol, further data detection would take place possibly utilising other modules that would be downloaded onto the end-user's computer.

With reference to figures 5 to 9, an alternative mode of operation using a control stub program is depicted. This mode of operation is similar to that described in connection with figures 1 to 4, except as outline below. With reference to figure 5, once the provider's URL button is pressed (step 202), a control stub will be downloaded to the user's computer (step 203) on the link 13 established between the provider's server 14 and the user's computer system 10.

With reference to figure 6, the stub code contains a secure Internet protocol that, once executed on the user's computer system, will establish a secure link 61 to the provider's data server 16 and retrieve a scanner component. The scanner component of the code runs (step 204) and establishes a link with the provider's data server from where it can call on program modules 62 necessary to detect the required data. The selection of these modules 62 will be dependent on the data items required to be detected, the operating system and age of the user's computer system 10.

With reference to figure 7, once the scan is complete, the detected data will be identified with a unique ID, possibly generated from session data, and then passed to the data server knowledge base 22 for verification (step 205). Confirmation of receipt of data will be passed back to the user's computer system (step 206).

With reference to figure 8, the configuration data is stored a transaction database 31 on the provider's server 16. Once confirmation is received by the user's computer system that the data has been stored correctly (step 206), the user will be invited to view the information detected. If the user chooses, the detecting / scanning software launches a new browser window (step 207) and displays a form containing the

BNSDOCID: <WO_____0225436A2_I_>

results. This form may be tailored to display the information selected by each client. The user will be invited to either confirm that the information is to be passed to the client or they will be given the opportunity to amend the information (step 207). The fields that the user has the option to amend may be controlled. Typically, they may include those where the data detected may conflict, for example, where the PC's manufacturer and model cannot be definitively detected, or where the PC has been re-badged or built under licence. The user may be given the opportunity to enter other information manually.

If any information presented in the user's form is altered, the revised information may be downloaded onto the provider's data server for audit purposes and preferably the client can be advised that the user elected to alter this information. If the user decides to edit the configuration data, a further communication may be commenced between the user's computer system and the provider's data server to complete this function (not shown). The user may then proceed, cancel or amend the configuration data (step 207)

If the action is to proceed, the user computer 10 sends a unique identification code for the information to the client web server on link 41 (step 208), and the client script uses this code to pull the scanning result from the provider's data server 16 on link 42 (step 209).

The present invention has been described in the context of specific embodiments. It will be understood that various modifications and adaptations are possible within the scope of the appended claims.

BNSDOCID: <WO_____0225436A2_I_>

CLAIMS

1. Apparatus for the remote scanning of configuration data relating to hardware or software installed in or as part of a user's computer system, the apparatus comprising:

means for downloading a software-based scanning module from a provider's server to a user's computer system;

said scanning module including means for determining preselected items of configuration data from the user's computer system and conveying said configuration data to the provider's server; and

means for forwarding said configuration data to a client server.

2. Apparatus according to claim 1 further including means for, remotely from the client server, preselecting required items of configuration data and storing said required items' definition in the provider's server.

3. Apparatus according to claim 2 wherein said means for remotely preselecting required items comprises a web page on the provider's server, accessible by the client.

4. Apparatus according to claim 1 in which the scanning module comprises means for detecting configuration data relating to hardware and/or software installed in, and/or peripherals connected to, said user's computer system.

5. Apparatus according to claim 1 further including means for initiating said downloading said scanning module comprising a URL embedded in a web page on said client server accessed by said user's computer system.

6. Apparatus according to claim 1 further including means for verifying the logical consistency of the configuration data collected from the user's computer system.

7. Apparatus according to claim 1 further including means for storing said configuration data for subsequent release to the client server.

BNSDOCID: <WO_____0225436A2_I_>

8. Apparatus according to claim 7 further including means to enable release of said configuration data to said client server, comprising means for providing to said user's computer system an identification code for transmission by said user's computer system to said client server, which code authorises release of said configuration data to said client server.

9. Apparatus according to claim 1 further including means for editing, by said user, configuration data transmitted to said provider's server, prior to forwarding said configuration data to said client server.

10. Apparatus according to claim 1 further including:

means for viewing, on said user's computer system, said configuration data determined from said user's computer system; and

means for authorising or inhibiting, by said user, transmission of said configuration data to said client server.

11. Apparatus according to claim 1 further including means, in said client server, for modifying a range of displayed options to the user's computer system, based on the determined configuration data for that user's computer system.

12. Apparatus according to claim 1 wherein said scanning module is adapted to collect only a sub-set of configuration data available at the user's computer system, according to a predetermined definition specified by a client server.

13. Apparatus according to claim 1 wherein said scanning module is adapted to automatically remove itself from the user's computer system after completion of the scanning operation.

14. Apparatus according to claim 1 wherein said scanning module comprises a plurality of scanning routines each adapted to call a further scanning routine dependent upon the configuration data determined.

BNSDOCID: <WO_____0225436A2_I_>

15. Apparatus according to claim 1 further including means for collecting data on usage of said scanning operations by user computer systems according to the client server from which initiation of the downloading originated.

16. Apparatus according to claim 1 further including means for initiating said downloading of at least one of a predetermined number of available scanning modules, said means for initiating comprising a plurality of URL's embedded in a web page on said client server accessed by said user's computer system, each of said URL's initiating downloading of a different scanning module.

17. Apparatus according to claim 1 further wherein said scanning module comprises at least one control stub adapted to call additional executable modules.

18. A method of remote scanning for configuration data relating to hardware or software installed in or as part of a user's computer system, the method comprising:

determining preselected items of configuration information required;

initiating, by a user, download of a scanning module from a provider's server to the user's computer system;

determining, by said scanning module, configuration data for said preselected items of configuration information from the user's computer system and conveying said configuration data to the provider's server.

19. The method of claim 18 further comprising authorising, by said user, transmittal of said configuration data to a client server.

20. The method of claim 19 wherein the step of determining preselected items of configuration required is effected remotely from said client server.

21. The method of claim 20 wherein the step of determining preselected items is effected via a web page on the provider's server accessed by the client server.

22. The method of claim 19 wherein the step of initiating download is effected from a user's computer system via a URL embedded in a web page on said client server.

BNSDOCID: <WO_____0225436A2_I_>

23. The method of claim 19 wherein the step of authorising transmittal is effected by said user's computer system issuing an identification code to said client server, which code authorises release of said configuration data, from said provider's server, to said client's server.

24. The method of claim 19 further including the step of automatically removing the downloaded scanning module from the user's computer system after completion of the scanning operation.

25. The method of claim 19 wherein the step of determining configuration data by said scanning module comprises the steps of downloading a succession of scanning routines, each successive scanning routine being selected and downloaded according to configuration data determined by a preceding scanning routine.

26. The method of claim 22 further including the step of providing a plurality of URL's embedded in web pages on the client server, each URL initiating downloading of a different scanning module.

27. A method of verifying compatibility of a user's computer system with at least one candidate product or service comprising the steps of:

visiting, by a user, a client web site;

initiating, by the user, download of a scanning module from a provider server to the user by activation of an address embedded in the client web site;

scanning the user's computer system using said scanning module;

forwarding configuration data resulting from the scan to the client server.

28. The method of claim 27 wherein the step of forwarding configuration data to the client server comprises the step of forwarding the configuration data to the provider server, and authorising release of the configuration data to the client server by said user.

BNSDOCID: <WO_____0225436A2_I_>

29. A system for detecting and forwarding, across the Internet to a third-party, configuration data detected from a user's computer, which user is a visitor to the third party's web site.

30. A system according to claim 29 in which said configuration data is detected by way of a software scanning module delivered over the Internet using standard transmission protocols.

31. A system according to claim 30 in which the scanning module comprises a plurality of scanning routines each adapted to call a further scanning routine dependent upon configuration data detected by a preceding scanning routine.

32. Apparatus substantially as described herein with reference to the accompanying drawings.

33. A method substantially as described herein with reference to the accompanying drawings.

BNSDOCID: <WO_____0225436A2_I_>

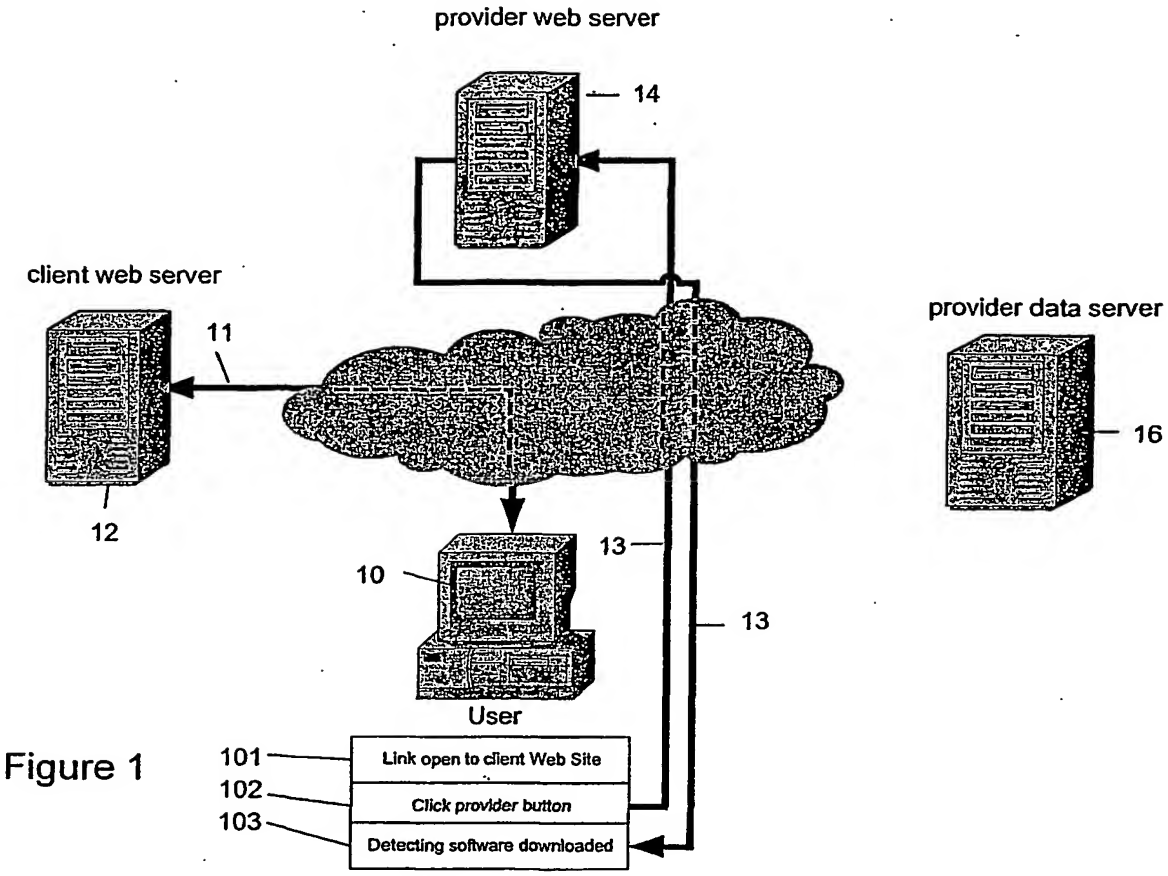

provider web server
14
client web server
11
provider data server
16
12
13
10
13
User
101
Link open to client Web Site
102
Click provider button
103
Detecting software downloaded

Figure 1

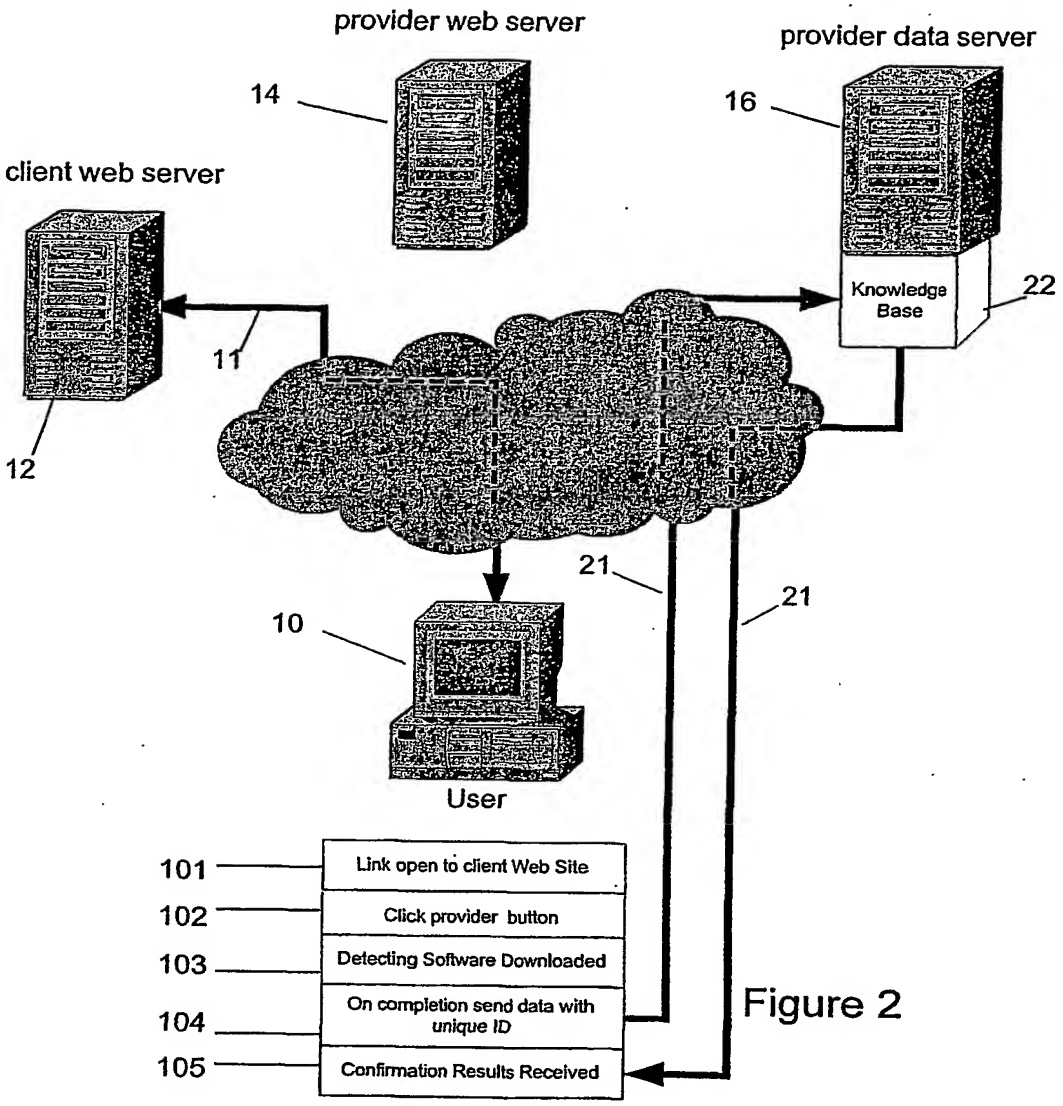
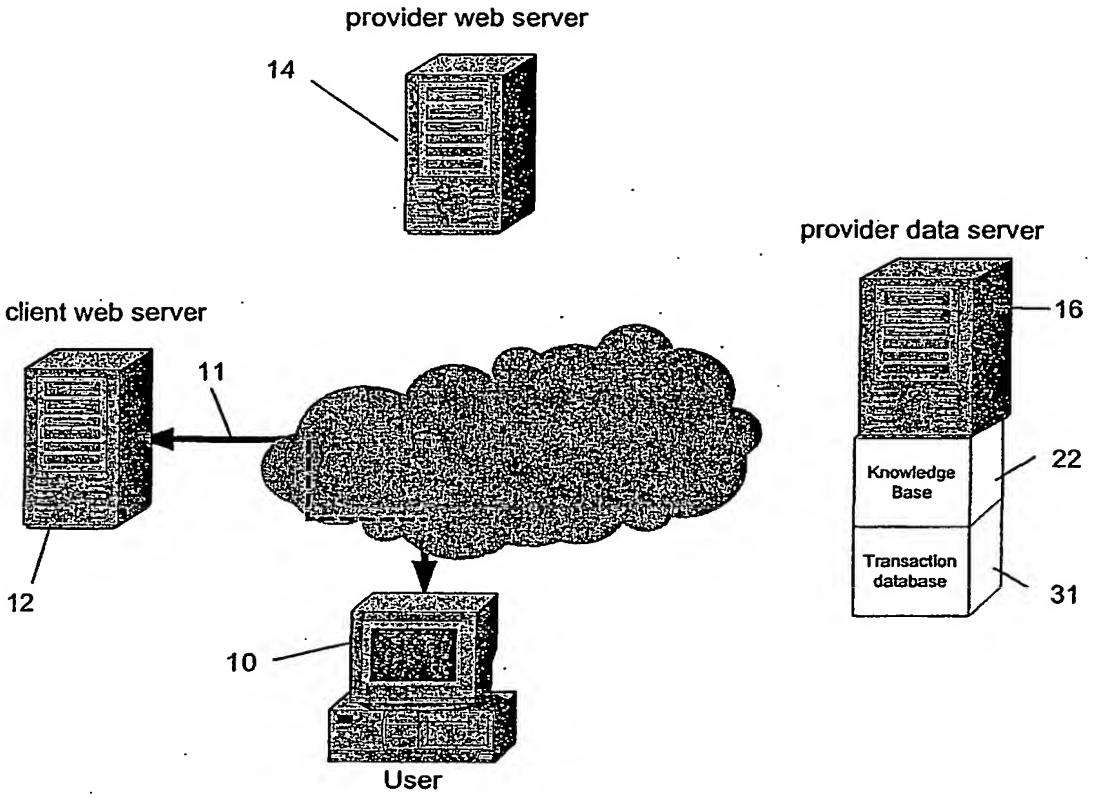

provider web server
provider data server
14
16
client web server
Knowledge Base
22
11
12
21
21
10
User
101
Link open to client Web Site
102
Click provider button
103
Detecting Software Downloaded
104
On completion send data with unique ID
105
Confirmation Results Received

Figure 2


provider web server
14
provider data server
client web server
16
11
Knowledge Base
22
Transaction database
31
12
10
User

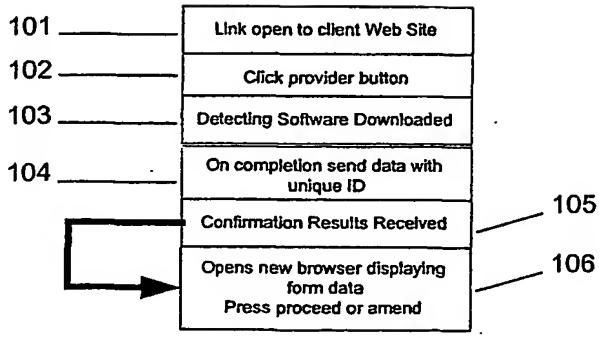

101
Link open to client Web Site
102
Click provider button
103
Detecting Software Downloaded
104
On completion send data with unique ID
Confirmation Results Received
105
Opens new browser displaying form data
Press proceed or amend
106

Figure 3

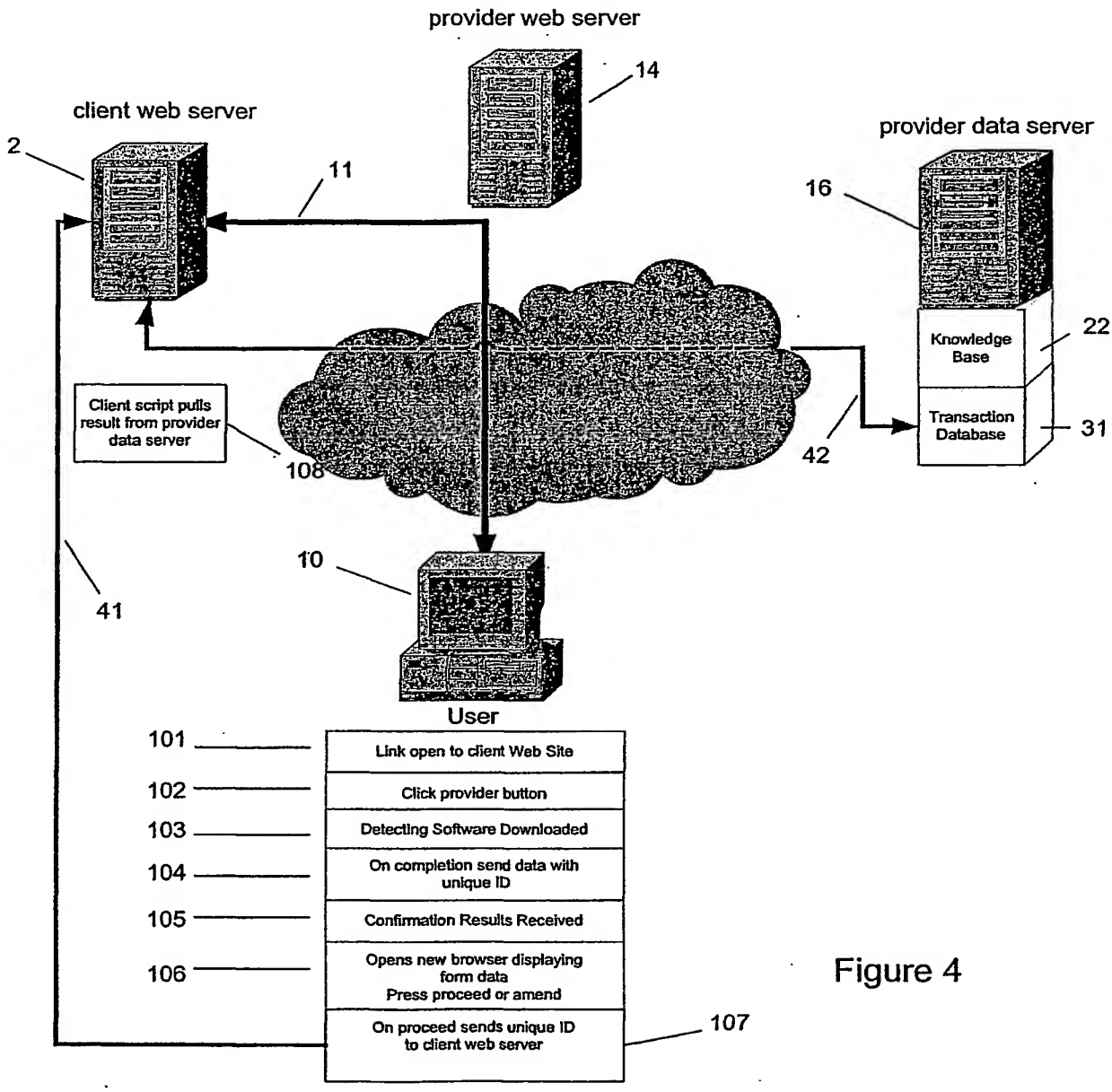

provider web server
14
client web server
2
11
provider data server
16
Knowledge Base
22
Transaction Database
31
Client script pulls result from provider data server
108
42
10
41
User
101
Link open to client Web Site
102
Click provider button
103
Detecting Software Downloaded
104
On completion send data with unique ID
105
Confirmation Results Received
106
Opens new browser displaying form data
Press proceed or amend
On proceed sends unique ID to client web server
107

Figure 4

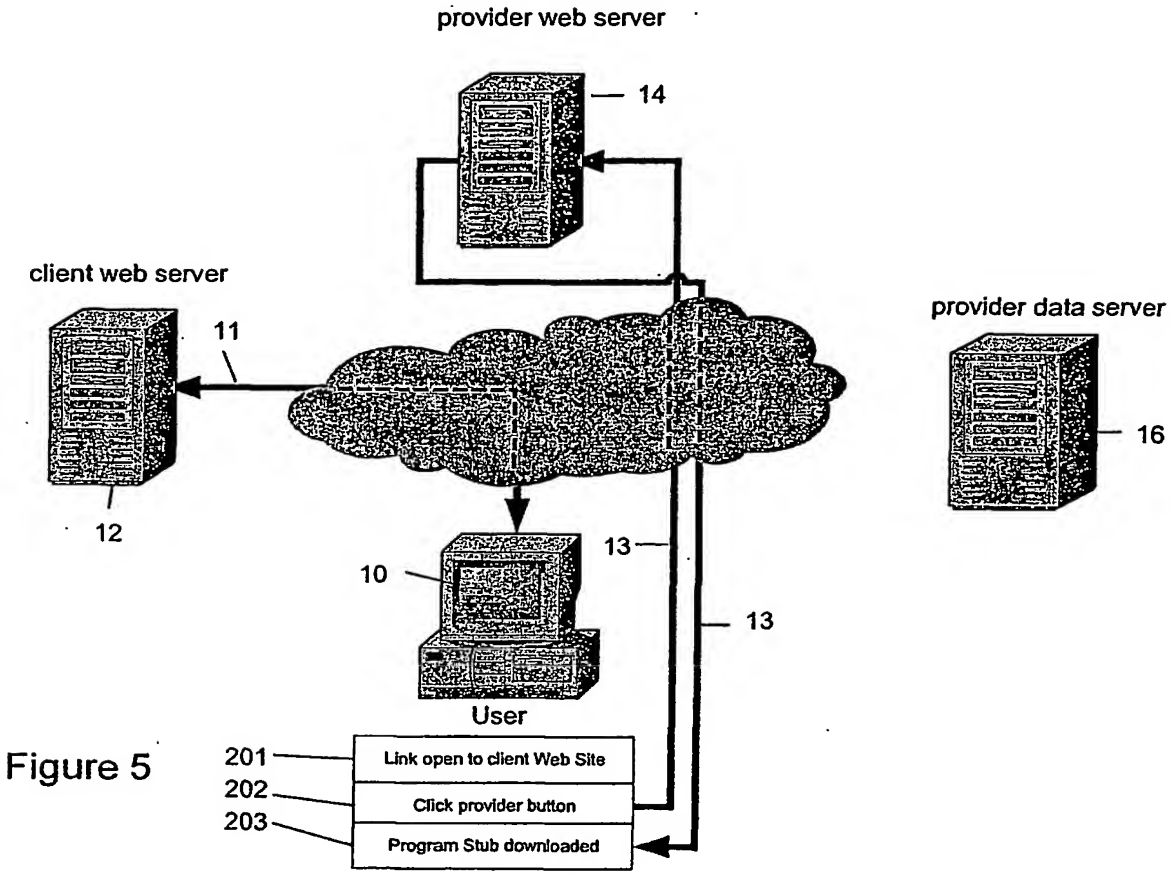

provider web server
14
client web server
11
provider data server
16
12
13
10
13
User
201
Link open to client Web Site
202
Click provider button
203
Program Stub downloaded

Figure 5

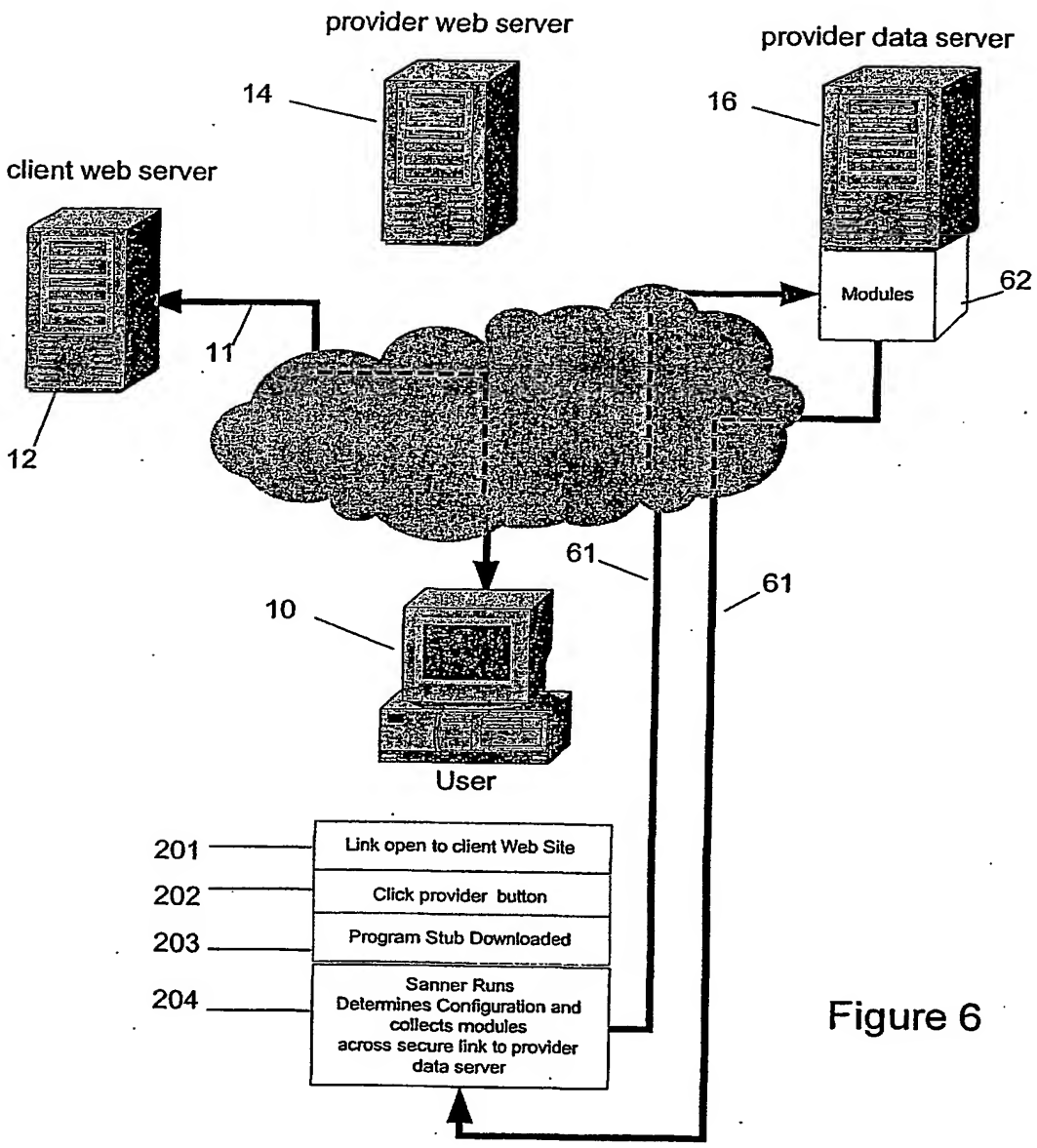

provider web server
provider data server
14
16
client web server
Modules
62
11
12
61
61
10
User
201
Link open to client Web Site
202
Click provider button
203
Program Stub Downloaded
204
Sanner Runs
Determines Configuration and
collects modules
across secure link to provider
data server

Figure 6

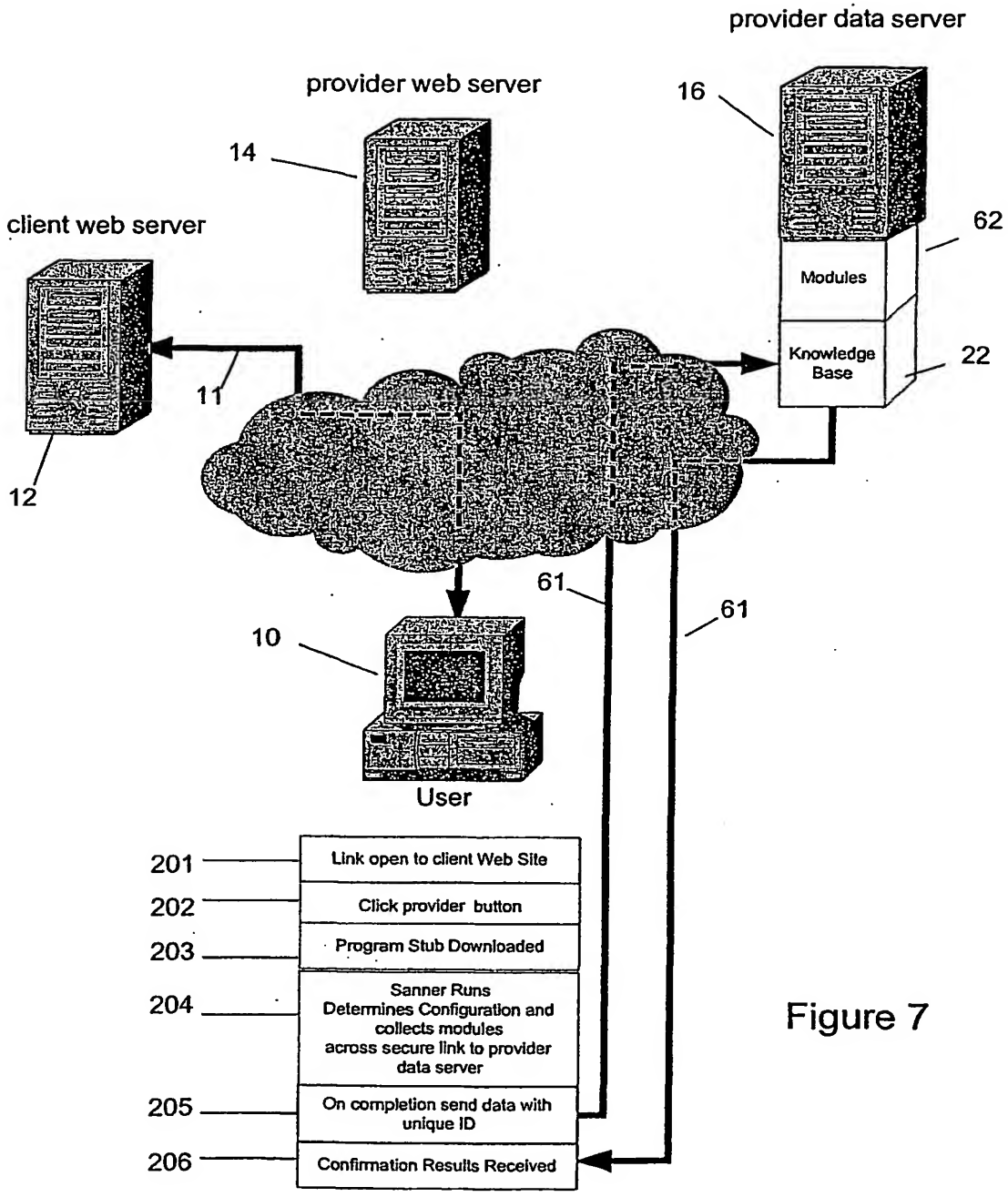
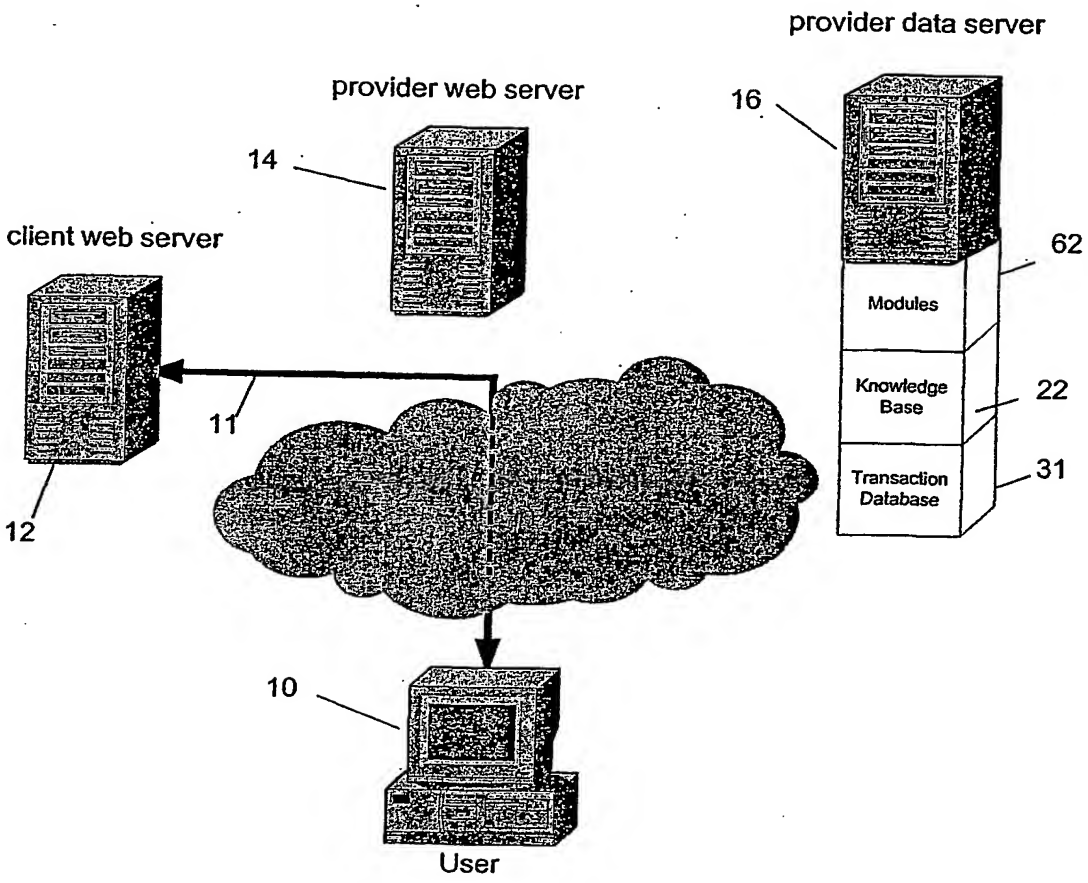

provider data server
provider web server
16
14
client web server
62
Modules
Knowledge Base
22
11
12
61
61
10
User
201
Link open to client Web Site
202
Click provider button
203
Program Stub Downloaded
204
Sanner Runs Determines Configuration and collects modules across secure link to provider data server
205
On completion send data with unique ID
206
Confirmation Results Received

Figure 7


provider data server
provider web server
16
14
client web server
62
Modules
Knowledge Base
22
Transaction Database
31
11
12
10
User

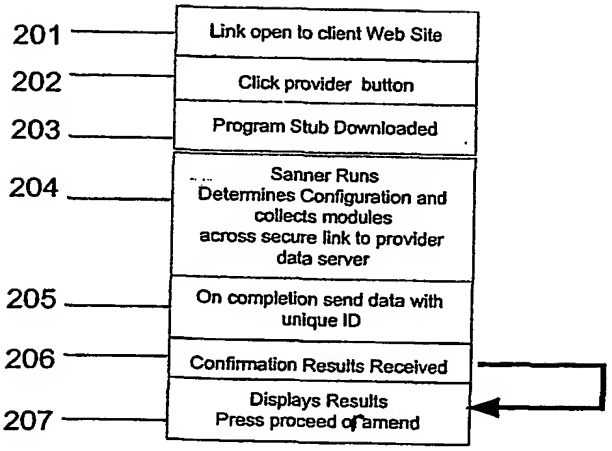

201
Link open to client Web Site
202
Click provider button
203
Program Stub Downloaded
204
Sanner Runs
Determines Configuration and collects modules across secure link to provider data server
205
On completion send data with unique ID
206
Confirmation Results Received
207
Displays Results
Press proceed or amend

Figure 8

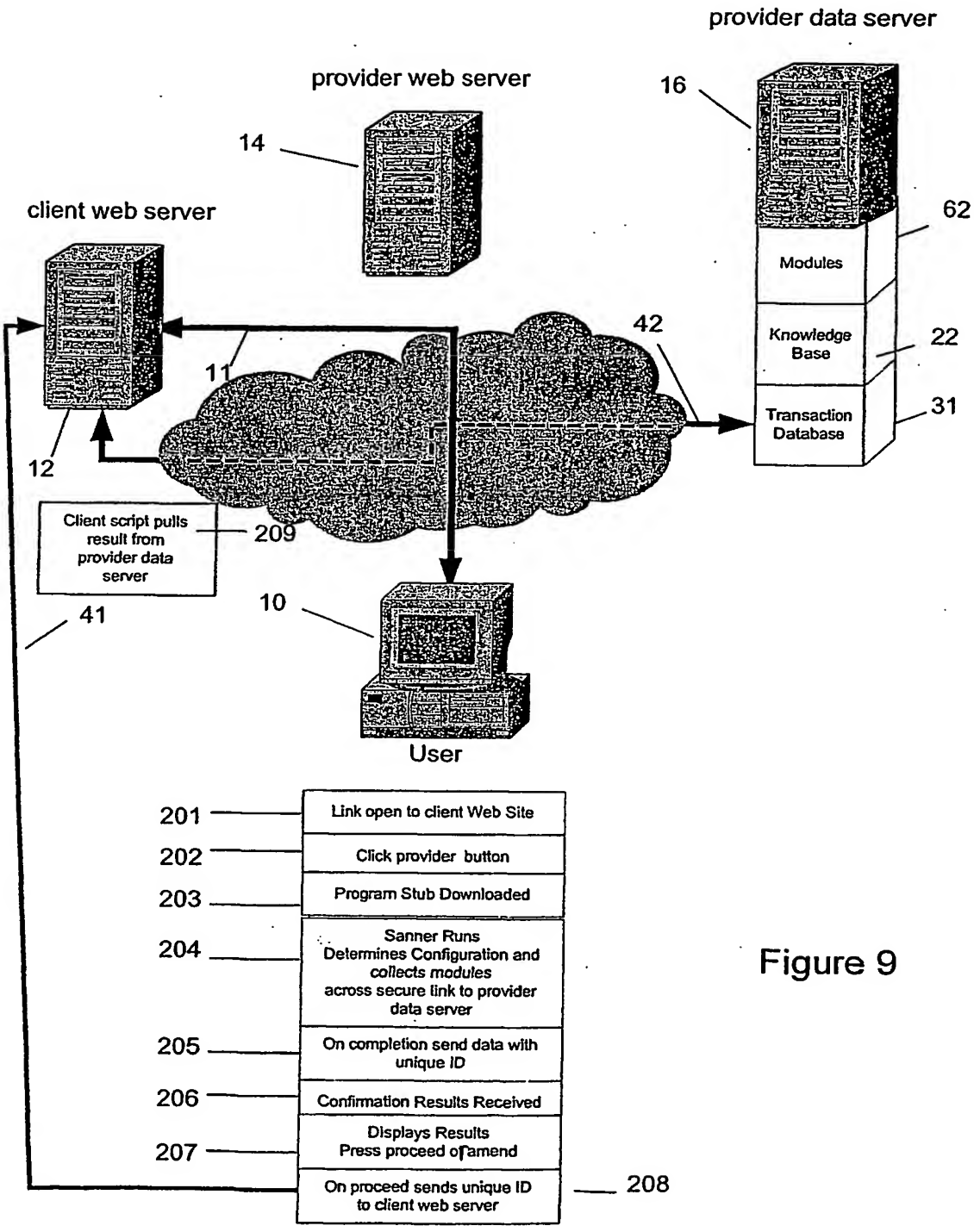

provider data server
provider web server
16
14
client web server
62
Modules
Knowledge Base
22
42
11
Transaction Database
31
12
Client script pulls result from provider data server
209
41
10
User
201
Link open to client Web Site
202
Click provider button
203
Program Stub Downloaded
204
Sanner Runs Determines Configuration and collects modules across secure link to provider data server
205
On completion send data with unique ID
206
Confirmation Results Received
207
Displays Results Press proceed or amend
On proceed sends unique ID to client web server
208

Figure 9

THIS PAGE BLANK (USPTO)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number
WO 02/025436 A3

(51) International Patent Classification[7]: G06F 9/445

(21) International Application Number: PCT/GB01/04174

(22) International Filing Date:
19 September 2001 (19.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0023177.9 21 September 2000 (21.09.2000) GB

(71) Applicant *(for all designated States except US)*: **WORK4SURE.COM LTD.** [GB/GB]; Millfield House, Cropwell Road, Radcliffe on Trent, Nottingham NG12 2JG (GB).

(72) Inventors; and

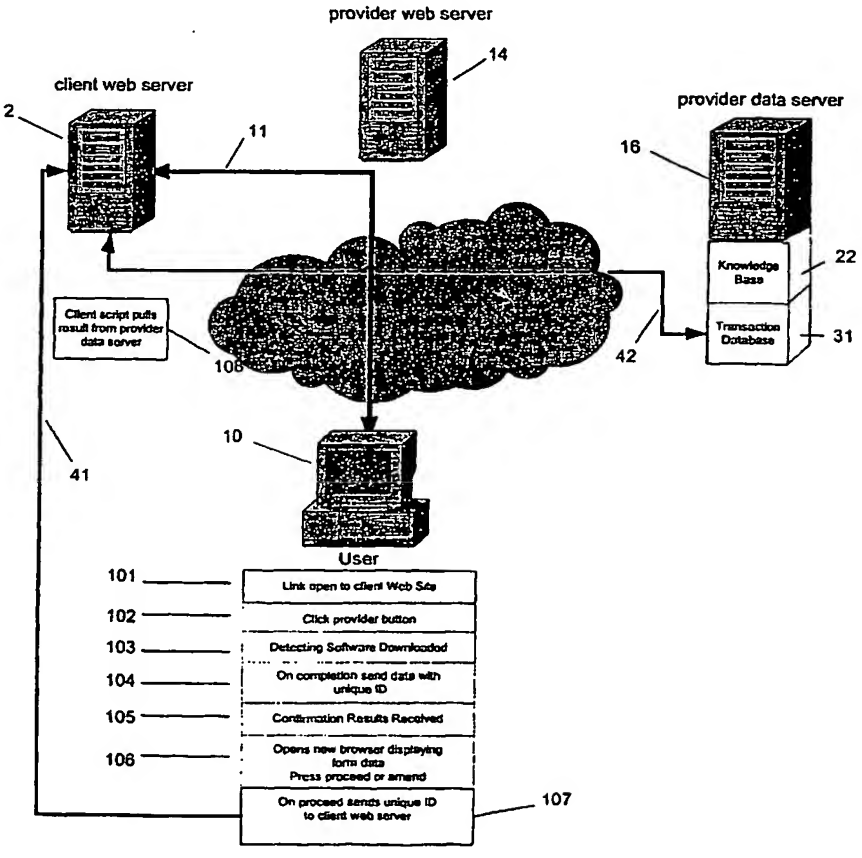
(75) Inventors/Applicants *(for US only)*: **MIRYANOV, Vitaly** [UA/GB]; 209 Sandycombe Road, Kew, Richmond, Surrey TW9 2EW (GB). **BATEMAN, Liam, Peter** [GB/GB]; 7 Shipps Close, Harleston, Norfolk IP20 9BG (GB). **FESSEY, Damian, Robert** [GB/GB]; Millfield House, 74 Cropwell Road, Radcliffe on Trent, Nottingham NG12 2JG (GB). **SHELDON, Andrew, David** [GB/GB]; Hall Barn, Westhorpe Road, Wyverstone, Suffolk IP14 4SP (GB). **LLOYD-ROACH, David, Joseph** [GB/GB]; 3 St. Mary's Walk, Ardley, Oxon OX27 7PR (GB).

(74) Agent: **CHARIG, Raymond, J.**; Eric Potter Clarkson, Park View House, 58 The Ropewalk, Nottingham NG1 5DD (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,

[Continued on next page]

(54) Title: REMOTE COMPUTER CONFIGURATION SCANNING



(57) Abstract: A system for detecting and forwarding, across the Internet to a third-party, configuration data detected from a user's computer, which user is a visitor to the third party's web site. In one configuration, apparatus for the remote scanning of configuration data relating to hardware or software installed in or as part of a user's computer system includes means for downloading a software-based scanning module from a provider's server to a user's computer system, the scanning module including means for determining preselected items of configuration data from the user's computer system and conveying said configuration data to the provider's server, and means for forwarding said configuration data to a client's server. The pre-selection of items of configuration data to be collected may be predetermined by the client to the provider. The user may be enabled to verify and authorise the forwarding of the information to the client's server by the provider's server.

WO 02/025436 A3

GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
8 August 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

national Application No
PCT/GB 01/04174

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 311 390 A (IBM) 24 September 1997 (1997-09-24) page 8, line 39 -page 10, last line	1,18,27
A	US 5 867 714 A (TERRELL MICHAEL R ET AL) 2 February 1999 (1999-02-02) column 5, line 55 -column 11, line 65	1-33
A	WO 00 36503 A (PCFIRST COM INC) 22 June 2000 (2000-06-22) column 3, line 18 -column 5, line 12	1-33
A	US 5 845 077 A (FAWCETT PHILIP E) 1 December 1998 (1998-12-01) column 5, line 29 - line 47	1-33

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 May 2002	22/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bijn, K

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/GB 01/04174

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00 52559 A (ISOGON CORP) 8 September 2000 (2000-09-08) page 8, line 25 -page 9, line 25	1-33

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

BNSDOCID: <WO_____0225436A3_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

national Application No
PCT/GB 01/04174

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2311390 A	24-09-1997	NONE	
US 5867714 A	02-02-1999	NONE	
WO 0036503 A	22-06-2000	AU 2481600 A	03-07-2000
		WO 0036503 A2	22-06-2000
US 5845077 A	01-12-1998	US 6073214 A	06-06-2000
		US 6327617 B1	04-12-2001
		US 2002016956 A1	07-02-2002
WO 0052559 A	08-09-2000	AU 3722300 A	21-09-2000
		WO 0052559 A1	08-09-2000

BNSDOCID: <WO_____0225436A3_I_>

THIS PAGE BLANK (USPTO)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)